ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №1

2020 წლის 16 ოქტომბერი

ქ. თბილისი

კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებამოსილებისა და საქმიანობის წესის დამტკიცების შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-8 მუხლის მე-5 პუნქტის, მე-11 მუხლის მე-2 პუნქტის „ა“ ქვეპუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, მე-13 მუხლის პირველი და მე-7 პუნქტების, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლის შესაბამისად, **ვბრძანებ:**

მუხლი 1

დამტკიცდეს „კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებამოსილებისა და საქმიანობის წესი“.

მუხლი 2

ძალადაკარგულად გამოცხადდეს „მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ“ მონაცემთა გაცვლის სააგენტოს თავმჯდომარის 2013 წლის 4 თებერვლის №5 ბრძანება.

მუხლი 3

ეს ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **გიორგი მეჟლუმიანი**

კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის უფლებამოსილებისა და საქმიანობის წესი

მუხლი 1. წესის მიზანი

ამ წესის მიზანია საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის – CERT.GOV.GE (შემდგომ – დახმარების ჯგუფი) საქმიანობის რეგლამენტაცია, დახმარების ჯგუფის უფლებებისა და მოვალეობების დადგენა, მესამე პირებთან დახმარების ჯგუფის ურთიერთობის პრინციპების განსაზღვრა, დახმარების ჯგუფის მიერ გაწეული მომსახურების სახეებისა და პირობების დადგენა, ასევე სხვა ამოცანების განსაზღვრა, რომელიც ემსახურება საქართველოში კიბერსივრცის უსაფრთხოების დაცვას.

მუხლი 2. დახმარების ჯგუფის მანდატი

1. დახმარების ჯგუფი CERT.GOV.GE წარმოადგენს ეროვნულ და სამთავრობო კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს (CERT), რომლის სამოქმედო უფლებამოსილება მოიცავს საჯარო დაწესებულებებისა და კერძო სექტორის ობიექტების დაცვას კიბერშეტევებისა და სხვა სახის კომპიუტერული ინციდენტებისაგან.

2. დახმარების ჯგუფის უფლებამოსილება არ ვრცელდება საიდუმლო ინფორმაციის მართვის, სისხლის სამართლის საქმეთა გამოძიების ან სამხედრო ოპერაციების სფეროზე, გარდა იმ შემთხვევებისა, როდესაც ამ სფეროთა უფლებამოსილი წარმომადგენლები თანამშრომლობენ დახმარების ჯგუფთან ერთობლივი საფრთხეებისა და ამოცანების გადაჭრის მიზნით.

3. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-9 მუხლის მე-5 პუნქტით გათვალისწინებულ შემთხვევაში, როდესაც მიმდინარე ან სავარაუდო კიბერშეტევა განსაკუთრებულ საფრთხეს უქმნის სახელმწიფოს თავდაცვისუნარიანობას, ეკონომიკურ უსაფრთხოებას, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალურ ფუნქციონირებას, დახმარების ჯგუფის თანამშრომელი შეიძლება, სააგენტოს თავმჯდომარის ბრძანებით, დაინიშნოს კომპიუტერული უსაფრთხოების სპეციალისტების საკოორდინაციო ჯგუფის ხელმძღვანელად, რათა ეფექტურად განხორციელდეს განსაკუთრებით სახიფათო ან/და მასშტაბური კიბერშეტევის თავიდან აცილება, მოგერიება ან/და მისი შედეგების აღმოფხვრა.

4. თუ სისხლის სამართლის საქმის ფარგლებში მიმდინარე გამოძიებისას დახმარების ჯგუფი ასრულებს კიბერშეტევის ანალიზს, დახმარების ჯგუფის წევრი უფლებამოსილია ჩვენება მისცეს სასამართლოში როგორც მოწმემ, საქართველოს სისხლის სამართლის საპროცესო კოდექსით დადგენილი წესით.

მუხლი 3. დახმარების ჯგუფის უფლებები და მოვალეობები

1. დახმარების ჯგუფი უფლებამოსილია, განახორციელოს საქართველოს კიბერსივრცის მონიტორინგი კომპიუტერული ინციდენტების გამოვლენისა და მართვის მიზნით, განსაზღვროს და გაატაროს კიბერუსაფრთხოების პოლიტიკა, წარმოადგინოს საქართველო ინფორმაციული და კიბერუსაფრთხოების საერთაშორისო ორგანიზაციებში და ღონისძიებებზე, ასევე განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებამოსილებები.

2. დახმარების ჯგუფის ფუნქციებია:

ა) კომპიუტერულ ინციდენტებზე რეაგირება და ინციდენტის მართვის პროცესის მხარდაჭერა, რაც მოიცავს:

ა.ა) კომპიუტერული ინციდენტების შესახებ შეტყობინებისა და მათი გაზიარების პლატფორმის შექმნასა და ადმინისტრირებას;

ა.ბ) კომპიუტერული ინციდენტების შესახებ შეტყობინების მიღებას;

ა.გ) კომპიუტერული ინციდენტების ანალიზს;

ა.დ)კომპიუტერულ ინციდენტებზე რეკომენდაციების გაცემას;

ა.ე) კომპიუტერულ ინციდენტებზე „არტეფაქტების“ მოპოვებასა და ექსპერტიზას;

ა.ვ) კომპიუტერულ ინციდენტებზე ანგარიშის შექმნას;

ა.ზ) კომპიუტერული ინციდენტების მართვის კოორდინაციას;

ბ) სხვადასხვა სამიზნე ჯგუფის ცნობიერების ამაღლების მიზნით ცოდნის და გამოცდილების გაზიარება, მათ შორის:

ბ.ა) საქართველოს კიბერუსაფრთხოების ფორუმის კოორდინაცია და ორგანიზაციული მხარდაჭერა;

ბ.ბ) კიბერუსაფრთხოების ცნობიერების ამაღლების კამპანიის მხარდაჭერა;

ბ.გ) ტრენინგების, სემინარებისა და საჯარო ლექციების ორგანიზება;

ბ.დ) ეროვნული კიბერსავარჯიშოების ჩატარება კერძო და საჯარო სექტორისთვის;

ბ.ე) ეროვნული კიბეროლიმპიადის ჩატარება სტუდენტებისთვის და სკოლის მოსწავლეებისთვის;

ბ.ვ) მოსალოდნელი საფრთხეების შესახებ საზოგადოებისა და ორგანიზაციების ინფორმირება;

ბ.ზ) სისუსტეების, საფრთხეებისა და განახლებების შესახებ ახალი ამბების მომზადება და საზოგადოების ინფორმირება სხვადასხვა არხის (მათ შორის, სოციალური ქსელის) საშუალებით;

გ) ინფორმაციული უსაფრთხოების ინციდენტების აღმოჩენა და მონიტორინგი, რაც გულისხმობს:

გ.ა) ქსელური სენსორების კონფიგურაციასა და მისი გამართულად ფუნქციონირების მხარდაჭერას;

გ.ბ) ქსელური სენსორების მონიტორინგს;

გ.გ) უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის (SIEM) სისტემის კონფიგურაციასა და მისი გამართულად ფუნქციონირების მხარდაჭერას;

გ.დ) უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის (SIEM) სისტემის მონიტორინგსა და ანალიზს;

გ.ე) სხვადასხვა ქსელური და სერვერულ-ინფრასტრუქტურული მოწყობილობის ჩანაწერების (ლოგფაილების) ანალიზს;

დ) ცალკეული ორგანიზაციებისა და სისტემების უსაფრთხოების სისუსტეების მართვა და მენეჯმენტი, რაც გულისხმობს:

დ.ა) სისუსტეების აღმოჩენასა და შესაბამისი კვლევების წარმოებას;

დ.ბ) სისუსტეების შესახებ საზოგადოებისა და სხვადასხვა ორგანიზაციის ინფორმირებას;

ე) კიბერუსაფრთხოების სფეროში აუდიტორული მომსახურება, რაც გულისხმობს:

ე.ა) ვებაპლიკაციების შეღწევადობის (პენეტრაციის) ტესტირებას;

ე.ბ) შიდა და გარე ქსელური ინფრასტრუქტურის შეღწევადობის (პენეტრაციის) ტესტირებას;

ე.გ) ქსელური მოწყობილობების კონფიგურაციის აუდიტს;

ე.დ) საწყისი პროგრამული კოდის ანალიზს;

ვ) კიბერუსაფრთხოების სფეროში მოქმედ საერთაშორისო და რეგიონულ ორგანიზაციებთან, უცხო ქვეყნის შესაბამის სტრუქტურებთან თანამშრომლობა, ინფორმაციის ურთიერთგაცვლა;

ზ) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის სერვერული ინფრასტრუქტურისა და აპლიკაციების ადმინისტრირება;

თ) სააგენტოს კიბერუსაფრთხოების უზრუნველყოფა, რაც გულისხმობს:

თ.ა) სააგენტოს ქსელური სენსორების კონფიგურაციას და მხარდაჭერას;

თ.ბ) სააგენტოს ქსელური სენსორების მონიტორინგსა და აღმოჩენას;

თ.გ) სააგენტოს ქსელური სენსორების მიერ გამოვლენილი შემთხვევების ანალიზს;

თ.დ) სააგენტოს უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის (SIEM) სისტემის კონფიგურაციასა და მხარდაჭერას;

თ.ე) სააგენტოს უსაფრთხოებასთან დაკავშირებული ინფორმაციისა და ხდომილებების მართვის (SIEM) სისტემის მონიტორინგსა და ანალიზს;

თ.ვ) სხვადასხვა ქსელური და სერვერული ინფრასტრუქტურული მოწყობილობების მიერ დაგენერირებული ჩანაწერების (ლოგფაილების) ანალიზს;

თ.ზ) სააგენტოს ვებაპლიკაციების შეღწევადობის (პენეტრაციის) ტესტირებას;

თ.თ) სააგენტოს შიდა და გარე ქსელური ინფრასტრუქტურის შეღწევადობის (პენეტრაციის) ტესტირებას;

თ.ი) სააგენტოს ქსელური მოწყობილობების კონფიგურაციის აუდიტს;

თ.კ) სააგენტოს მიერ წარმოებული საწყისი პროგრამული კოდის ანალიზს.

3. თავისი საქმიანობის განხორციელებისას, დახმარების ჯგუფი ხელმძღვანელობს პრიორიტეტული საფრთხეებით, რომელიც დადგენილია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-8 მუხლის მე-2 პუნქტით, ასევე საქართველოს კიბერუსაფრთხოების სტრატეგიითა და სამოქმედო გეგმით.

4. ამ მუხლით დადგენილი ფუნქციების ფარგლებში სააგენტომ შესაძლოა დაინტერესებულ მხარეს გაუწიოს მომსახურება წინასწარ დადებული წერილობითი ხელშეკრულების საფუძველზე და ხელშეკრულების განსაზღვრულ ფარგლებში. გადაუდებელ შემთხვევებში მომსახურების გაწევა შესაძლებელია ზეპირი შეთანხმების საფუძველზე, რომლის შედეგადაც შემდგომში უნდა დაიდოს წერილობითი ხელშეკრულება.

მუხლი 4. ურთიერთობა კრიტიკული ინფორმაციული სისტემის სუბიექტთან

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის III თავის მოთხოვნათა დაცვით, კრიტიკული ინფორმაციული სისტემის სუბიექტთან დახმარების ჯგუფის ურთიერთობის სტანდარტულ ფორმატს წარმოადგენს კონტაქტი აღნიშნული სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტთან.

2. თუ დახმარების ჯგუფი ან/და კრიტიკული ინფორმაციული სისტემის სუბიექტი საჭიროდ ჩათვლის, დახმარების ჯგუფისა და კომპიუტერული უსაფრთხოების სპეციალისტის ურთიერთობა ხორციელდება დაცული კავშირის, დაშიფრული გზავნილების ან/და ინფორმაციის დაცვის სხვა საშუალებებით.

3. დახმარების ჯგუფის მოთხოვნა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომაზე განსახილველად მიეწოდება სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერს. დახმარების ჯგუფის მოთხოვნაზე პასუხის გაცემის (რეაგირების) ვადა განისაზღვრება სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის შეთანხმებით.

4. კომპიუტერული უსაფრთხოების სპეცილისტის ან ინფორმაციული უსაფრთხოების მენეჯერის ხელმიუწვდომლობის შემთხვევაში კრიტიკული ინფორმაციული სისტემის სუბიექტმა უნდა განსაზღვროს შემცვლელი თანამშრომელი (თანამშრომლები), რომელსაც მიეცემა გადაუდებელი ღონისძიებების განხორციელების უფლებამოსილება.

5. ამ მუხლით განსაზღვრული, ასევე სხვა დაკავშირებული საკითხების განსაზღვრის მიზნით, სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტს შორის შესაძლებელია გაფორმდეს თანამშრომლობის მემორანდუმი.

მუხლი 5. კომპიუტერული ინციდენტის მართვა

1. საქართველოს სამთავრობო ქსელის მონიტორინგის შედეგად გამოვლენილი, ქსელური სენსორების

ქსელის მართვის დროს აღმოჩენილი, ქართული და უცხოეთის ორგანიზაციებიდან მიღებული ან სხვაგვარად დახმარების ჯგუფისათვის უშუალოდ მიწოდებული ინციდენტების მართვას ახორციელებს უშუალოდ დახმარების ჯგუფი.

2. კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში მომხდარი ან სავარაუდო ინციდენტის იდენტიფიცირებას ახორციელებს სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი. კომპიუტერული უსაფრთხოების სპეციალისტის მიერ ინფორმაციულ სისტემაში არსებული მოვლენის კომპიუტერულ ინციდენტად იდეტნტიფიცრების შემთხვევაში, ვალდებულია ამგვარი ინციდენტის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდოს დახმარების ჯგუფს.

მუხლი 6. დასკვნითი დებულებები

1. თუ კრიტიკული ინფორმაციული სისტემის სუბიქტი, სხვა სახელმწიფო ორგანო ან კერძო ორგანიზაცია ქმნის შინასამსახურებრივ CERT ჯგუფს, დახმარების ჯგუფის აღნიშნულ CERT ჯგუფთან ურთიერთობა რეგულირდება ამ წესების მე-5 მუხლით.

2. საქართველოს სამართალდამცავ ორგანოებთან უფლებამოსილების გამიჯვნის, გამოძიებაში დახმარების გაწევის, საექსპერტო დახმარების, ინციდენტების მართვისა და სხვა მნიშვნელოვანი საკითხები ფორმდება თანამშრომლობის მემორანდუმით.